

FG 设置案例手册

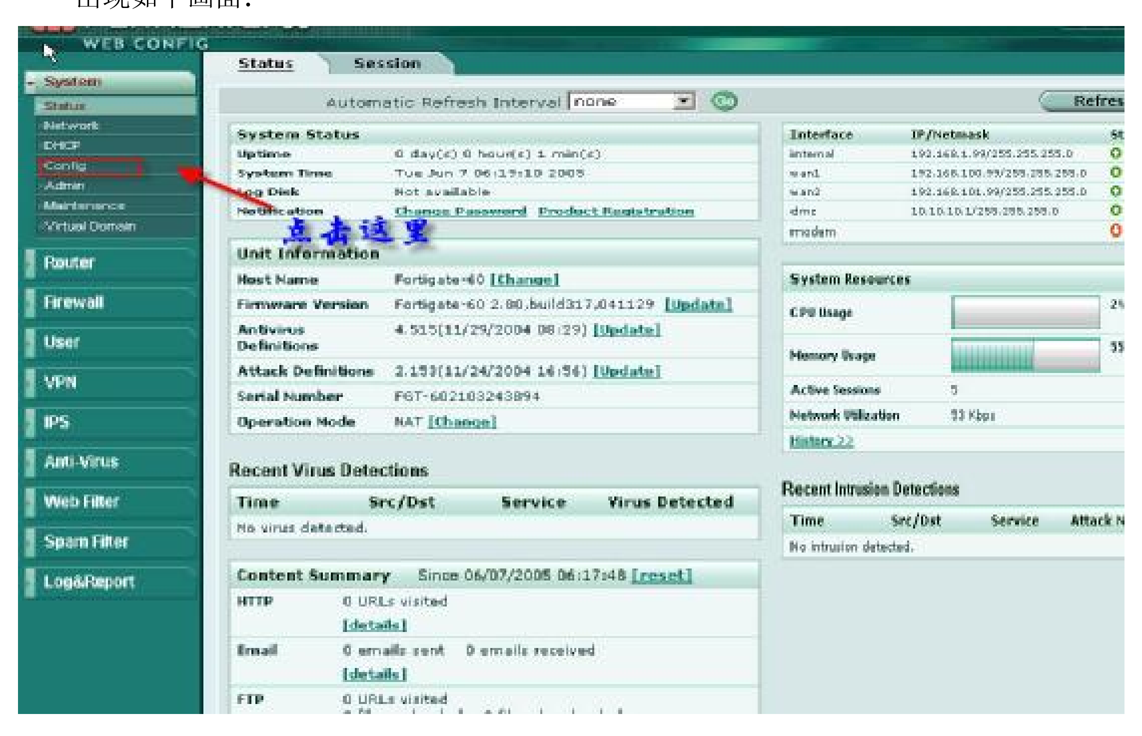
V.28051223

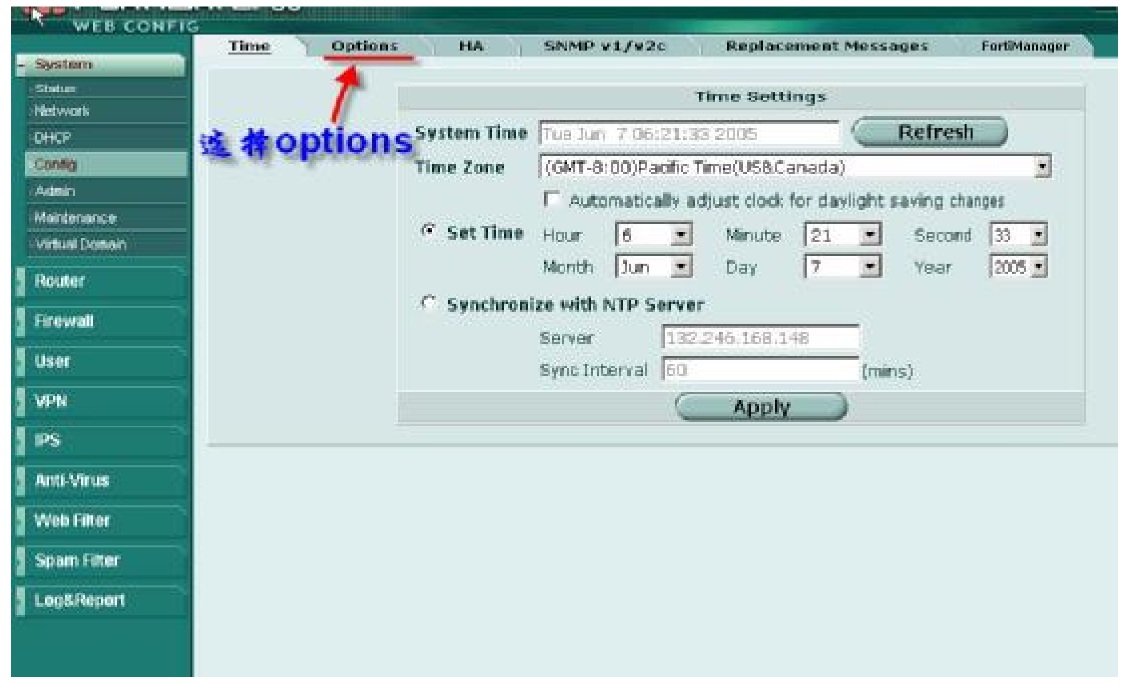
漆金生
Jinsheng Qi
上海华盖科技发展有限公司福州办事处
Shanghai Huagai&Technology Developmet Co.,LTD. Fuzhou Office
地址：福州市五一中路状元街 99 号汇福花园 3 座 403 室
ADD:3-403/Room,Community of Huifu garden ,No.99 of Zhuangyuan Road,FuZhou
电话/Tel：+86 591 83360512   传真/FAX：+86 591 83360621   http://www.huagai.com

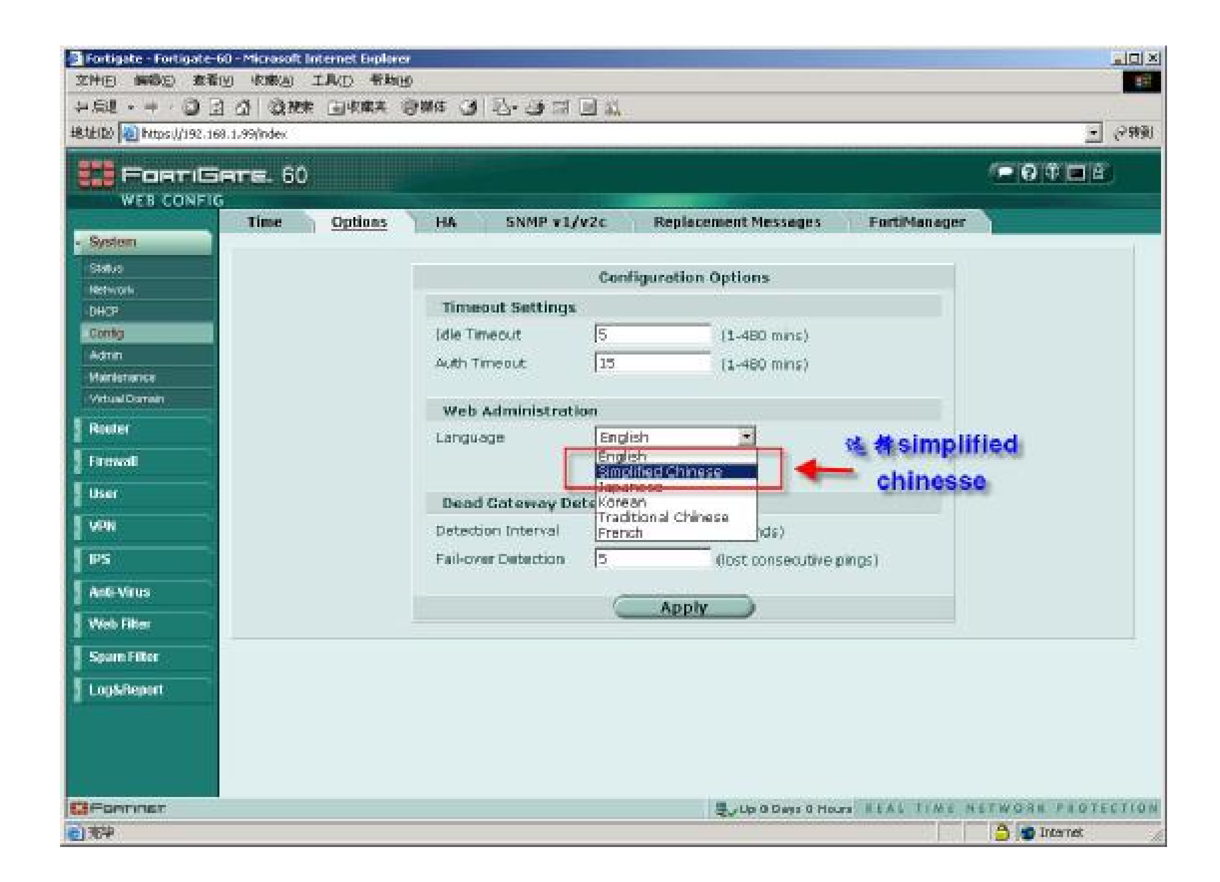
一，　　更改语言：

在 IE 中输入 https://192.168.1.99 (防火墙默认 IP)

出现如下画面：







点击 Apply，就可以转换成简体中文。

二、配置网络接口：

登录方法一样，如下图：



1，内网 IP 设置：

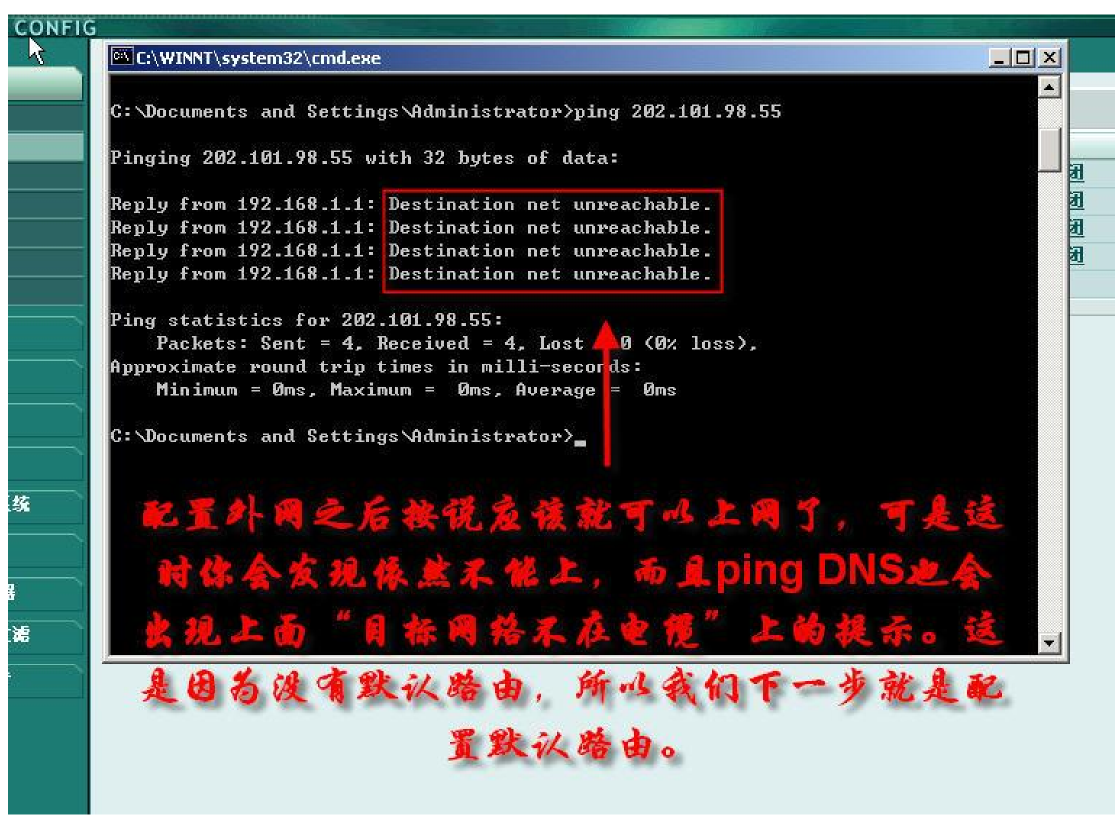

接口
区
DNS
调制解调器
新建
名称
IP地址
网络掩码
访问选项
状态
internal 192.168.1.99 255.255.255.0 HTTPS,PING,HTTP 关闭
wan1 192.168.100.99 255.255.255.0 PING 关闭
wan2 192.168.101.99 255.255.255.0 PING 关闭
dmz 10.10.10.1 255.255.255.0 HTTPS,PING 关闭
modem
状态
DHCP
路由
防火墙
设置用户
虚拟专网
入侵检测系统
病毒检查
点击这里配置局域网

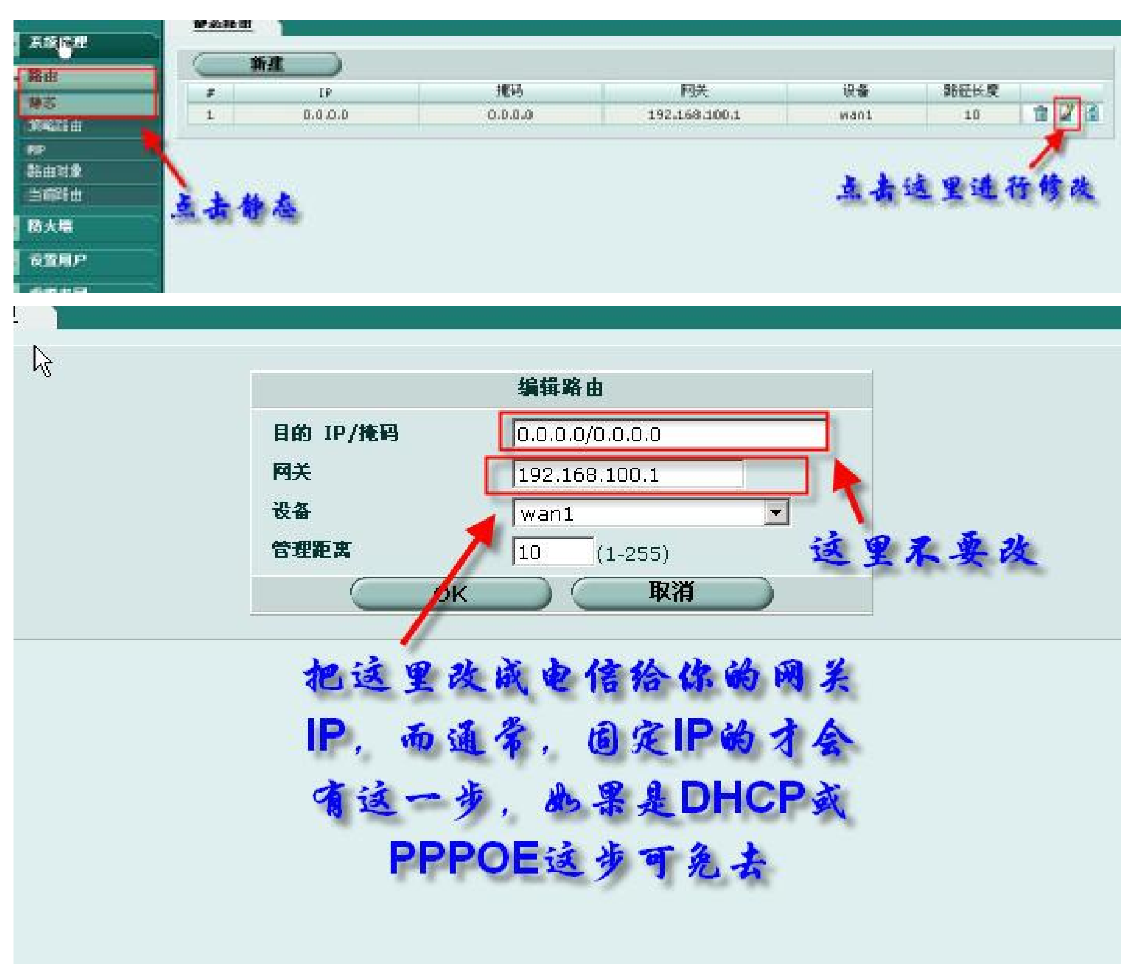

WEB CONFIG
接口
区
DNS
调制解调器
系统管理
状态
网络
DHCP
配置
管理员设置
维护
虚拟域
路由
防火墙
设置用户
虚拟专网
入侵检测系统
病毒检查
Web 过滤器
垃圾邮件过滤
端口编辑/VLAN
接口名称
internal (00:09:0F:0A:9C:D0)
地址模式
自定义
DHCP
PPPoE
IP地址/网络掩码: 192.168.1.99/255.255.255.0
DDNS
启用
Ping服务器
启用
管理访问
HTTPS
PING
HTTP
SSH
SNMP
TELNET
MTU
分解大于MTU的输出包. 1500 (字节)
日志
OK
取消
跟据需要
配置内网
接口地址
跟据需要打
开相关管理


新建
名称
IP地址
网络掩码
访问选项
状态
internal 192.168.1.1 255.255.255.0 HTTPS,PING,HTTP 关闭
wan1 192.168.100.99 255.255.255.0 PING 关闭
wan2 192.168.101.99 255.255.255.0 PING 关闭
dmz 10.10.10.1 255.255.255.0 HTTPS,PING 关闭
modem
系统管理
DHCP
配置
管理员设置
维护
虚拟域
路由
防火墙
设置用户
点击这里配置外网IP

2，外网静态 IP 配置：


接口
区
DNS
调制解调器
系统管理
状态
网络
DHCP
配置
管理员设置
维护
虚拟域
路由
防火墙
设置用户
虚拟专网
入侵检测系统
病毒检查
Web 过滤器
垃圾邮件过滤
日志与报告
跟内网配置一样，跟据需要进行配置
端口编辑/VLAN
接口名称
wan1 (00:09:0F:0A:9C:D2)
地址模式
自定义
DHCP
PPPoE
IP地址/网络掩码:
192.168.100.99/255.255.255.0
DDNS
启用
Ping服务器
启用
管理访问
HTTPS
PING
HTTP
SSH
SNMP
TELNET
MTU
分解大于MTU的输出包,
1500
(字节)
日志
OK
取消


CONFIG
C:\WINNT\system32\cmd.exe
C:\Documents and Settings\Administrator>ping 202.101.98.55
Pinging 202.101.98.55 with 32 bytes of data:
Reply from 192.168.1.1: Destination net unreachable.
Reply from 192.168.1.1: Destination net unreachable.
Reply from 192.168.1.1: Destination net unreachable.
Reply from 192.168.1.1: Destination net unreachable.
Ping statistics for 202.101.98.55:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Administrator>
配置外网之后按说应该就可以上网了，可是这时你会发现依然不能上，而且ping DNS也会出现上面“目标网络不在电缆”上的提示。这是因为没有默认路由，所以我们下一步就是配置默认路由。



3，外网动态 IP PPPOE 配置：

接口名称 external (00:09:0F:50:C0:E3)

地址模式

○ 自定义 ○ DHCP ◉ PPPoE

用户： [redacted]@fzlan

密码： *******

无编号IP：

初始化Disc超时： 1

初始化PADT超时： 1

管理距离： 1

☑ 从服务器中重新得到网关.

☐ 改变内部DNS.

☑ 连接到服务器 （状态: 失败）

此项先中之后，默认路由不用更改！

DDNS ☐ 启用

Ping服务器 ☐ 启用

管理访问 ☐ HTTPS ☑ PING ☐ HTTP ☐ SSH ☐ SNMP ☐ TELNET

MTU ☑ 分解大于MTU的输出包. 1492 （字节）

日志 ☐

OK 取消

通常，如果是 PPPOE，一般不需要设置默认路由。

三、　设置端口转发：

FG 防火墙虚拟 IP 功能提供三种服务：

静态 NAT：这是个一对一的关系，既，一个外部地址对应一个内部地址，而这个外部地址必须是在地址池中，且必须是当前没有在用的。如果你防火墙只有一个公网 IP，此项服务将不能应用。

端口转发：是指把外部网络发往防火墙外部接口上的某个端口上的数据，全部转发到内部网络中某个 IP 上，这个 IP 的接收端口可以和转发端口一样，也可以不一样，以实现内部网络某项服务可以向外网发布或提供。这篇文档所要描述的就是这个内容。

动态端口转发：跟端口转发类似，只是不指定外部 IP 地址，让防火选择任意外部 IP 进行转发。当防火墙是动态 IP 的时候，可以选择此项服务。

注意：虚拟 IP 最多只能设置 1024 个。

现在假设，我内部有一台 WEB 服务器，在不使用 DMZ 的情况下，需要向外部网络发布。我的外部网络是：192.168.22.0/24,内部网络是：192.168.1.0/24,并且指定防火墙外网 IP 为 192.168.22.17/24，所以只能选择端口转发。（出于安全的考虑，跟据权限最小化原则，在不是特别情况下，请尽量使用端口转发）下面就是这个操作的过程：

1、 进入“防火墙→虚拟 IP→新建”，所填内容如下图所示：



注：1,名称可随意写，主要是为管理方便起到标识做用。本处因为是要对外发布 WEB 服务，所以，用“WEB”来标识。外部接口选择外网接入的接口既可。

2,当需要使用动态端口转发时，在外部 IP 地址处输入：0.0.0.0

3,因为防火墙的管理端口目前还不能更改，所以在启用 80 端口进行转发的时候，请一定关闭或不要开启防火墙的 HTTP 的管理端口，如下图：



2、 进入“防火墙→策略→新建”，新建一条从外到内的策略，如下图：



3、 验证设置是否正确，从外网访问 http://192.168.22.17, 如图：



至此，设置已全部完成，如果还需要开放其他端口，设置方法一样。注意，FG 端口转发目前不能连续开放一系列端口，既是说，您如果要在同一 IP 上开放多个端口，那么只能一个个加上相关虚拟 IP 端口转发和相关对应的策略。如果开放的实在多，那么建意还是使用 DMZ，并通过在策略里面选择相应的服务组来一次性开放。

四、IP MAC 绑定设置：

IP/MAC 绑定可以保护 FG 设备和企业网络不受 IP 欺骗的攻击，这样可以有效的保护企业内部网络恶意者为了超越权限上网或对 FG 设备的设置进行更改而任意改变自己电脑 IP 的问题。

FG IP/MAC 有 DHCP 自动分配和手动两种方式，而 DHCP 分配目前只支持 50 对的绑定。

现在假设，我们只允许内部网络中绑定了 IP/MAC 地址的电脑上网和访问 FG 设备。下面我们就这两种方式来分别进行配置。

1， DHCP 方式

1．1　在接口上启用 DHCP 服务。进入“系统管理→DHCP→服务”选择接口点击“修改”图标，如下图：



注：我们是想在内部网络中使用 IP/MAC 绑定，所以选择“internal”点击红色箭头所指图标。



注：因为这一步在默认情况下就是打开的，所以，一般情况下，你可以跳过一步。

1．2　修改分配 IP 地址范围。进入“系统管理→DHCP→服务器”，同样点击编辑图标，得到如下图：

编辑DHCP服务器

名称 internal_dhcp_server
接口 internal
域
缺省网关 192.168.1.99
IP范围 192.168.1.110 - 192.168.1.210
掩码 255.255.255.0
租期 无限
7 (天) 0 (小时) 0 (分钟)
(5 分钟 - 100 天)
DNS服务器 1 192.168.1.99
DNS服务器 2
DNS服务器 3
WINS服务器 1
WINS服务器 2
可选 1 代码: 0 可选:
可选 2 代码: 0 可选:
可选 3 代码: 0 可选:
OK 取消

注：一般只修改 IP 地址范围，其余地方可跟据具体情况修改，也可以按默认不变。

说明：1.1 和 1.2 两个步骤默认情况下都是开启的，可以不用设置直接进入下面的步骤。

1.3 进行 IP/MAC 绑定。进入“系统管理→DHCP→IP/MAC 绑定”点“新建”，得到下图：



注：名称可跟据使用者编写，方便管理就行；IP 地址一定要是 1.2 步中，所写 IP 地址范围之内的。MAC 地址就填写使用者电脑 MAC。这里我们新建了两对，如下图：

名称	IP地址	MAC地址	
jin	192.168.1.112	00:d0:59:15:33:23	
jingshne	192.168.1.116	00:d0:59:15:33:27	

1.4　　设置策略使用的地址。进入“防火墙→地址→地址”点新建，如下图：



注：地址名称和 IP 地址一定要写刚才在 IP/MAC 绑定时所写的名字和地址，此处的掩码是：255.255.255.255；刚才所建 IP/MAC 的所有地址对，都要如是新建出来，如下：

jin	192.168.1.112
jingshne	192.168.1.116

1.5　　设置地址组。进入“防火墙→地址→组”点新建，如下图：



1．5　设置由内而外的策略。进入“防火墙→策略”点编辑图标，得到如下图：



注：把地址名改为刚才新建的地址组，其余可不变。

1.6 在 telnet 中启用绑定功能。在 CMD 中，输入：telnet 192.168.1.1(防火墙内网 IP 地址，如下图操作：

```
Fortigate-50A login: admin
Password:
Welcome !

Fortigate-50A # get firewall ipmacbinding setting
bindthroughfw       : disable
bindtofw            : disable

Fortigate-50A # config firewall ipmacbinding setting

(setting)# set bindthroughfw enable

(setting)# set bindtofw enable

(setting)# set undefinedhost block

(setting)# end

Fortigate-50A # get firewall ipmacbinding setting
bindthroughfw       : enable
bindtofw            : enable
undefinedhost       : block

Fortigate-50A # config system interface

(interface)# edit internal

(internal)# set ipmac enable

(internal)# end

Fortigate-50A # show system interace in
command parse error before 'interace'

Fortigate-50A # show system interface internal
config system interface
    edit "internal"
        set dhcp-server-mode server
        set ip 192.168.1.99 255.255.255.0
        set allowaccess ping https telnet
        set ipmac enable
    next
end

Fortigate-50A #
```

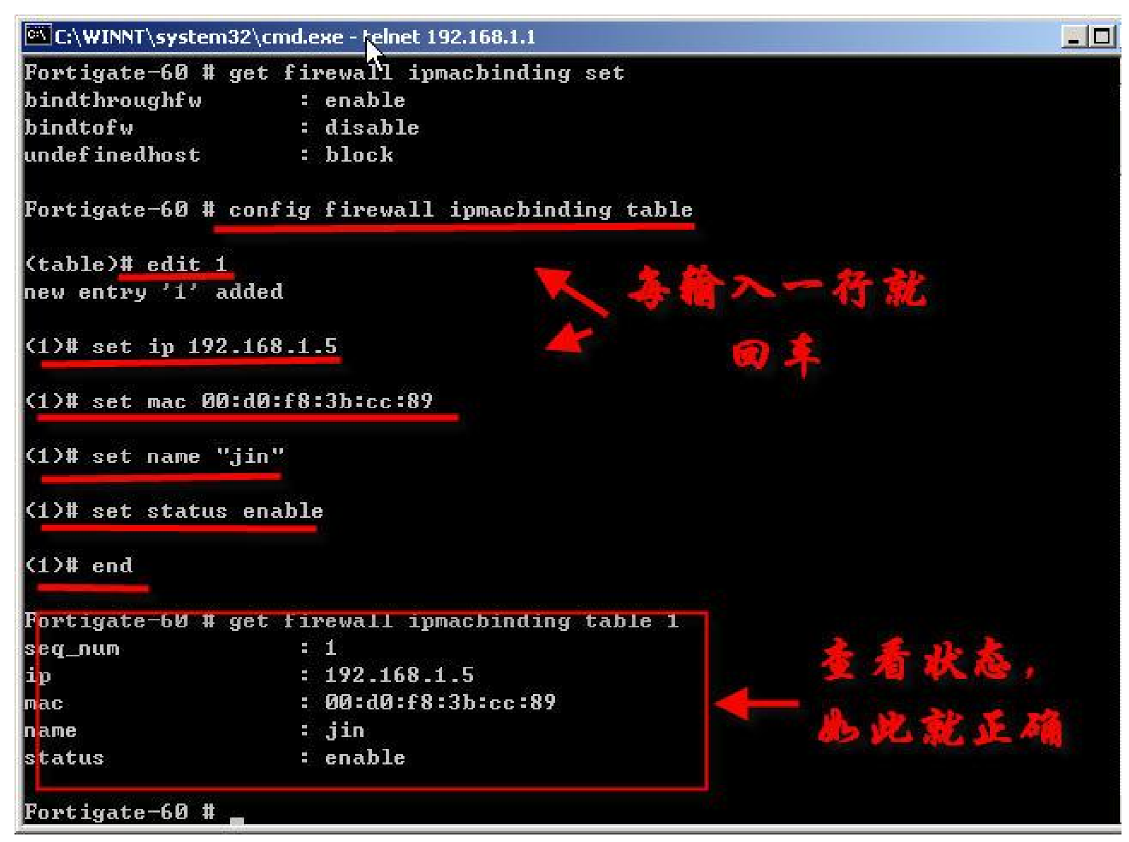
注：第一个红框中由上往下三个设定的意思分别为，充许绑定的 IP 穿透防火墙；充许绑定 IP 到达防火墙；没有绑定的全部阻止。

第二个红框中的意思在接口上启用绑定功能。

到此我们就完成了全部的设置，这个时候，没有绑定的 IP，无论他怎么改，他都无法上网和访问防火墙本身。

2，手动方式

手动方式跟 DHCP 分配大部分地方是相同的，唯一不一样的地方，就是 DHCP 中的 1.3 步不一样，在手动方式中，这一步也是在 TELNET 中设置的，所以，只要把下面这一步跟上面的 1.3 步替换掉就行，当然 1.1 1.2 这两步也就不用考虑了。如下图：



注：当有多个绑定的时候，每编辑完一个，都要“END”，然后“EDIT 2….EDIT N”一直到全部写完为此。

五、PPTP VPN 服务设置

在 FG 中，PPTP 服务有两种，一是 PPTP 服务器，一是 PPTP 服务穿透。
PPTP 服务器：是客户端直接向 FG 拔号，并由 FG 进行验证和解封装。
PPTP 服务穿透：是指 FG 只转发 PPTP 数据包到 FG 后面的 PPTP 服务器。

现在假设，我的外部网络为 192.168.22.0/24 段，内部网络为 192.168.1.0/24 段。

1， PPTP 服务器设置

1．1 为拔入的 PPTP 客户端设置验证用户名和密码。进入 “设置用户→本地”点击新建,得到如下图并填写用户名和密码,点确定.



注:有多少用户就建多少用户.

1．2 设置用户组.进入 “用户设置→用户组” 点击新建,得到如下图:



注:在我们刚新建的可用成员中,选中所用来验证 PPTP 的,全部推入红框中所在地方.组

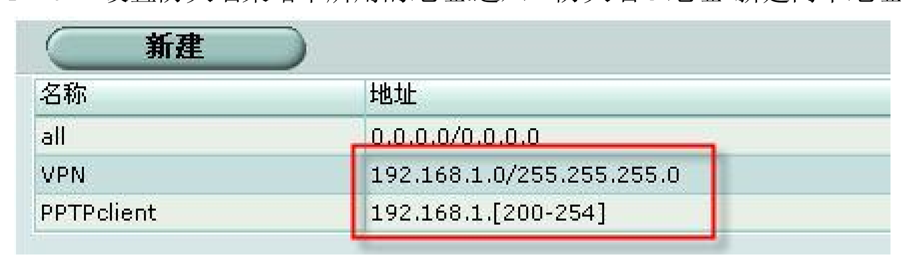
名可以任意写.

1．3　激活 PPTP 服务器.进入＂虚拟专网→PPTP”,红框中所示内容:



注:起始 IP 和终止 IP 为分配给 PPTP 客户端拔入时用的 IP 队列,此 IP 队列必须是内网中没有在用的.用户组选择 1.2 中新建的组名.做完这一步,客户端这时已经可以拔入上来了,但是不能做任何的访问.因为防火墙在没有定义什么流量可以通行之前,默认情况下,是阻止所有流量的.所以,我们必须进行下一步骤,定义可以通行的流量.

1．4　设置防火墙策略中所用的地址.进入“防火墙→地址”新建两个地址:


新建

名称	地址
all	0.0.0.0/0.0.0.0
VPN	192.168.1.0/255.255.255.0
PPTPclient	192.168.1.[200-254]

注:VPN 为内网需要让拔入客户端访问的地址;PPTPclient 为分配给拔入端的地址,也可以说是在 1.3 中的 IP 队列.当然,名字可以任意取.

1．5　设置防火墙由外而内的策略.进入“防火墙→策略”点击新建,如下图:



注:源地址是不是可以选 “ALL”?其实是可以的,但是从安全的角度考虑,还是建议不要做这做.

至此,PPTP服务器设置已经全部完成.

2， 设置PPTP服务穿透.

这里主要有两个步骤,基本上跟做端口转发一样,这里就不做详细叙述.

2.1 定义一个TCP1723 的端口转发(PPTP端口)

2.2 设置防火墙策略,充许定义的流量到刚才新建的虚拟IP上.

再次感谢您选择上海华科技发展有限公司为您提供产品和服务，希望我们有更多合作机会。如果您有任何疑问或建意，欢迎来电、来信，E-mail:hxl@huagai.com 。